APPENDIX E

ALARM MANAGEMENT GUIDANCE

(PROGRAMMATIC AND FACILITY)

TABLE OF CONTENTS

RECORD OF REVISIONS

Rev	Date	Description	POC	OIC
0	11/17/03	Initial issue.	Mel Burnett, FWO-DECS	Gurinder Grewal, FWO-DO

RESPONSIBLE ENGINEERING STANDARDS POC AND COMMITTEE
for upkeep, interpretation, and variance issues

Section D3060/F1050 App E	Instrumentation & Controls POC/Committee

1.0   PURPOSE

This appendix provides guidance for assigning alarms to process monitoring and control systems and for implementing an alarm management strategy.

2.0   SCOPE

A method is provided to assign, prioritize, and document the basis of alarms used in the operation of a process facility. Fire alarms, security system alarms, and radiation alarms are not addressed. The design basis for controls and interlocks is not provided.

The methodology in this chapter is highly recommended for safety-related alarm systems and for basic process control systems in non-reactor nuclear, high and medium-hazard non-nuclear facilities.

3.0   ACRONYMS AND DEFINITIONS

3.1   ACRONYMS

CLD – Control Logic Diagrams

CLI – Component Location Identifier

DCS – Distributed Control System

DHEC – Department of Health and Environmental Control

EN – Equipment Number

OSR – Operational Safety Requirement

PHR – Process Hazards Report

P&ID – Process & Instrumentation Diagram

PLC – Programmable Logic Controller

SAR – Safety Analysis Report

3.2   DEFINITIONS

Advisory – Information within the normal realm of operation that should be brought to the operator's attention, but does not require immediate operator action. Such information usually includes the maintenance status of plant equipment, automated systems, and interlocks.

If the operator is expected to determine an abnormal condition as part of his normal surveillance, then the condition should be presented to the operator as advisory information. As a Rule of Thumb, if transition of a process condition from normal to abnormal takes more than 30 minutes, an operator should detect it during normal surveillance. In general, advisories do not actuate a horn or buzzer.

Alarm – A process condition that requires operator notification so that action can be initiated by the operator to avert personal injury, equipment damage, safety and technical specification violations, environmental releases, or loss of function to process or safety systems.

Alarm Avalanche – An alarm avalanche condition occurs when a process event results in an overwhelming number of alarms. Such a condition usually makes it difficult or impossible for operating personnel to determine the nature of the event and to respond appropriately.

Alarm Prioritization Criteria – A set of established criteria used to classify an alarm based on the potential severity or impact of the alarm condition in a given process facility.

Alarm Review Team (ART) – Representatives from Engineering and Operations organizations assigned to review and approve alarm and interlock selection.

Alarm Selection Worksheet – A worksheet used to identify and document process alarms and their justification.

Alarm Validation Process – A systematic method for ensuring that alarm functions are properly selected and implemented.

Alert – Time dependent information indicating a trend in which lack of operator action could develop into an alarm condition. In general, alerts do not actuate a horn or buzzer.

Common Trouble Alarm – An alarm based on two or more abnormal conditions within the process. The alarm is usually triggered by the first of the abnormal conditions that occurs and returns to normal only after all abnormal conditions have cleared.

Guideline for Alarms – A set of practices to be followed in the identification and assignment of facility / process alarming functions.

Interlock – A process condition for which a process monitoring and control system takes automatic action to avert personal injury, equipment damage, safety and technical specification violations, environmental releases, or loss of function to process or safety systems.

If the operator does not have sufficient time to interpret an abnormal condition and take the required action, then an interlock should be configured in lieu of an alarm. As a Rule of Thumb, a process interlock should be considered for any transient from normal to abnormal conditions which takes less than 5 minutes, and should be required if it takes less than 2 minutes.

Multiple-Alarm-Event – A plant state that causes several alarm conditions to occur in a very short time period.

4.0   ALARM IDENTIFICATION AND PRIORITIZATION

A. Alarms are typically assigned in a process facility during design, although additional alarms are often added during commissioning, startup, and operations. Many alarms and interlocks are configured for specific facility, system, or component modes of operation. The resulting number of alarms presented to the operator may be excessive. Computer automation has exacerbated the situation by making it very easy to add new or change existing alarms. Too many alarms can lead to nuisance or redundant alarms, alarm avalanche conditions, or alarms that provide little or no assistance to operating personnel.

B. An alarm validation process should be used to assign, configure, prioritize, and document the basis of alarms and interlocks in a process facility. This process should be implemented in stages to review and document the basis for both new and existing alarms / interlocks and define the scope of recommended improvements to the current alarm management system.

C. An Alarm Review Team should be appointed to develop and implement the alarm validation process. The review team should consist of members representing both the operations and engineering organizations. The alarm validation methodology and the resulting recommendations should be approved by the review team, engineering, and operations management to insure that there is consistency between the current operating strategy, technical and safety requirements, and alarm response procedures.

D. One member of the Alarm Review Team should be assigned as the Alarm Validation Coordinator. The Alarm Validation Coordinator coordinates the activities of the team; tracks candidate alarms and interlocks through the evaluation; maintains records of the review results and recommendations; and submits results to project management and operations for review and approval of design, set point, and procedure changes resulting from the validation process.

E. The first step in the alarm validation process involves the identification of candidate and existing alarms / interlocks based on a review of the current technical baseline. The process then consists of documenting the justification, establishing set points, and establishing the method of detecting and responding (i.e. operator intervention vs. automatic interlock) to the event or condition. Instrument loops should be reviewed from a systems perspective to support existing alarms or recommend the addition or deletion of alarms. Process alarms and interlocks should be assigned as part of a facility monitoring and control strategy through an established Guideline for Alarms. The Guideline for Alarms should be developed to incorporate the accepted facility / industry standards and practices for implementing and handling alarms of generic process systems and alarm types. The following is an example of a typical set of guidelines that might be used for assigning alarms:

   1. Assign alarms only where the process operator must take a specific action directed to the process. Alarm response actions to "call someone" or some similar activity should not be used as a basis for an alarm. An alarm should not merely be informative (e.g., just to make sure the operator is aware of something).

   2. Assign alarms only for abnormal conditions over which the operator has control and / or responsibility.

   3. Delete unnecessary and redundant alarms if the process operator is already aware of the abnormal condition that led to the alarm. Specifically, if the answer to the following questions is "yes", the alarm is considered redundant:

      a. Is the operator already aware of the situation through normal surveillance activities?

      b. Is the operator already aware of the situation through other alarms and interlocks?

      c. Has the appropriate operator action been taken due to other alarms or interlocks?

   4. If an abnormal event of process origin (not including power failures, loss of instrument air, and the like) will generate two or more alarms, then consider the use of a common trouble alarm to address the multi-alarm event.

5. Assign alarms based on the following operator expectations:

   a. If the transition of a process variable from near normal to abnormal is unlikely to happen within 30 minutes, then the process operator is expected to detect the situation as a part of normal surveillance activities.

   b. If the alarm requires action by the operator in less than 5 minutes after the alarm condition is generated, then a process interlock or other automatic mechanism of response should be implemented in lieu of an alarm.

6. Suppress alarms that are not meaningful during specific operation or maintenance modes.

F. For facilities with many alarms, Alarm Prioritization Criteria should be established that reflects the relative severity of the condition or event indicated by an alarm. Priority levels should be established to reflect the importance of various alarm conditions in a given process facility. Each alarm should be assigned a priority based on the criteria. The alarm priorities can then be incorporated into the facility's alarm management system and procedures to assist operating personnel in identifying and responding to the most critical alarms. The following is an example of a typical set of Alarm Prioritization Criteria that might be used.

Priority 1 Alarm – Priority 1 alarms should warn operators of the most significant events requiring operator action. These alarms are generally safety based, however, depending on the nature of the process facility they may be based on critical regulatory, product quality, or economic criteria. For example, in a nuclear process facility, a Priority 1 Alarm might be used to warn the operator that there is a potential for a significant release of radioactivity or hazardous chemical that might affect the health and safety of employees and the general public. Alarms of this priority usually necessitate the manual shutdown of the process.

Priority 2 Alarm – Priority 2 alarms should warn the operator of less significant events than Priority 1 Alarms. As an example, these events could indicate the potential for transition to an unsafe condition, exceeding a regulatory or quality limit, or interrupting process operation. Priority 2 Alarms usually require action by the operator to mitigate the condition while maintaining process operation.

Priority 3 Alarm – Priority 3 alarms should warn the operator of less significant events than Priority 2 alarms. As an example, these events might include the potential to damage equipment, interrupt process operation, and/or exceed product quality limits. Alarms of this priority are based primarily on economic impact and require operator intervention to avoid a shutdown, equipment repair, etc.

Alert – An Alert provides an indication to the operator that the process is approaching an alarm condition, which may be avoided by appropriate operator action. Typically return-to-normal corrections are made through routine operations and procedures.

Advisory – An Advisory indicates a failure or status change that does not impact the ability to continue normal operation in a safe manner. No operator action is required.

G. Once alarms have been identified and prioritized, an Alarm Validation Process should be applied to determine whether an alarm, interlock, or advisory is appropriate based on the time and information available for an operator to respond to an abnormal condition. This criteria addresses facility specific issues such as the need for hardwired alarms / interlocks, the use of automatic versus manual action, and handling multiple alarm conditions.

5.0　ALARM VALIDATION PROCESS

A.　The implementation of a detailed alarm validation process can be established through the performance of the following steps. A Flowchart is proved as an attachment to this appendix (Attachment 1) to provide a graphic representation of the validation process.

Step 1:　Review pertinent technical documentation for alarm and interlock requirements. These may include P&IDs, CLDs, Loop Sheets, System Design Descriptions, Software Requirement Specifications, Set Point Documents, SARs, PHRs, OSRs, Process Requirements, DHEC and DOE requirements.

Step 2:　Apply the Guideline for Alarms to determine what alarms / interlocks are required for the process system, see Item E in Section 4.0 above.

Step 3:　Identify candidate alarms, interlocks, and set-point values noting the process system, instrument number (EN or CLI), instrument loop description, and type of installation (e.g., DCS, PLC, or Hardwired).

Step 4:　Apply the Alarm Prioritization Criteria developed for the facility, see Item F in Section 4.0 above.

Step 5:　Determine if Priority #1 alarm criteria is satisfied. If so and the alarm /interlock is part of or impacts the operation of a safety function, then it is recommended that implementation results in a highly reliable design.

Step 6:　Determine if Priority #2 alarm criteria is satisfied.

Step 7:　Determine if Priority #3 alarm criteria is satisfied.

Step 8:　Determine if only an Alert is needed. If so, proceed to the last step.

Step 9:　Determine if only an Advisory is needed. If so, proceed to the last step.

Step 10:　If the answers to Steps 5 through 9 are all "No" and notification currently exists, then it is recommended that the notification be removed from the facility.

Step 11:　If the answer to Steps 5, 6, or 7 is "Yes", then it should be determined whether the alarm is required for only certain modes of operation. If so, the alarm should be linked with operational mode criteria to mask the alarm when it is not valid. An example would be when a low flow alarm is provided for a pump, the alarm would be masked or blocked when the pump was not running.

Step 12: If an interlock is provided to respond to an abnormal condition due to operational preferences or human limitations, the following items should be considered in the justification of a Priority #1, #2, or #3 alarm.

1. Refer to the P&IDs, CLDs, and Guideline for Alarms to assist in evaluating the requirement for the interlock. If it is determined that an interlock is required but has not been implemented for an existing process / facility, then compensatory measures should be placed into effect until the interlock is incorporated. If no interlock is required then an alarm is valid.

2. If an interlock exists and the operator can take action to correct the abnormal condition before the interlock occurs, then the alarm is valid. The interlock may not be necessary and should be considered for removal. As a Rule Of Thumb, an operator usually needs at least 5 minutes to recognize an abnormal condition and take action. If operator action cannot prevent the interlock, then justification for the alarm needs further consideration.

3. If the operator is required to take additional actions after an interlock occurs to lessen the severity of an event or to provide immediate notification of the event, then an alarm is valid. If no operator action is required, then an Alert or Advisory indication should be considered.

Step 13: If an abnormal condition generates two or more alarms, the alarms may be considered redundant. Examples of redundant alarms are:

1. Two or more alarms from redundant field instruments that monitor the same process variable.

2. Two or more alarms from independent field instruments that monitor process related variables.

3. Two or more alarms from field instruments that monitor independent process variables that exceed their alarm limits in rapid succession, as a result of one particular abnormal event condition.

Note: The criteria for alarm redundancy should not be applied to loss of power, instrument air, or other loss of service conditions that in general are multi-alarm events.

If the alarm is determined to be redundant, a determination should be made to see if a single common alarm could replace two or more redundant alarms. Examples of grouped ("ganged") alarms are:

1. A common Low Tank Temperature Alarm and a common High Tank Temperature Alarm.

2. A common Loss of Flame Alarm.

3. A common Filter Plugging Alarm.

Step 14: Create a common alarm based on the redundant alarms. If redundant alarms are needed as advisory information for the operator, classify them as Advisories.

Step 15: Document the alarm functionality and required operator alarm response.

B. Alarm Selection Worksheets are recommended to maintain a record of the alarm validation process and to document the design basis for new alarms and changes to the current alarm configuration resulting from the application of the validation process. A typical example of an Alarm Selection Worksheet along with Instructions is provided as an attachment to this appendix (Attachment 2).

Attachment 1: Alarm Validation Process Flowchart
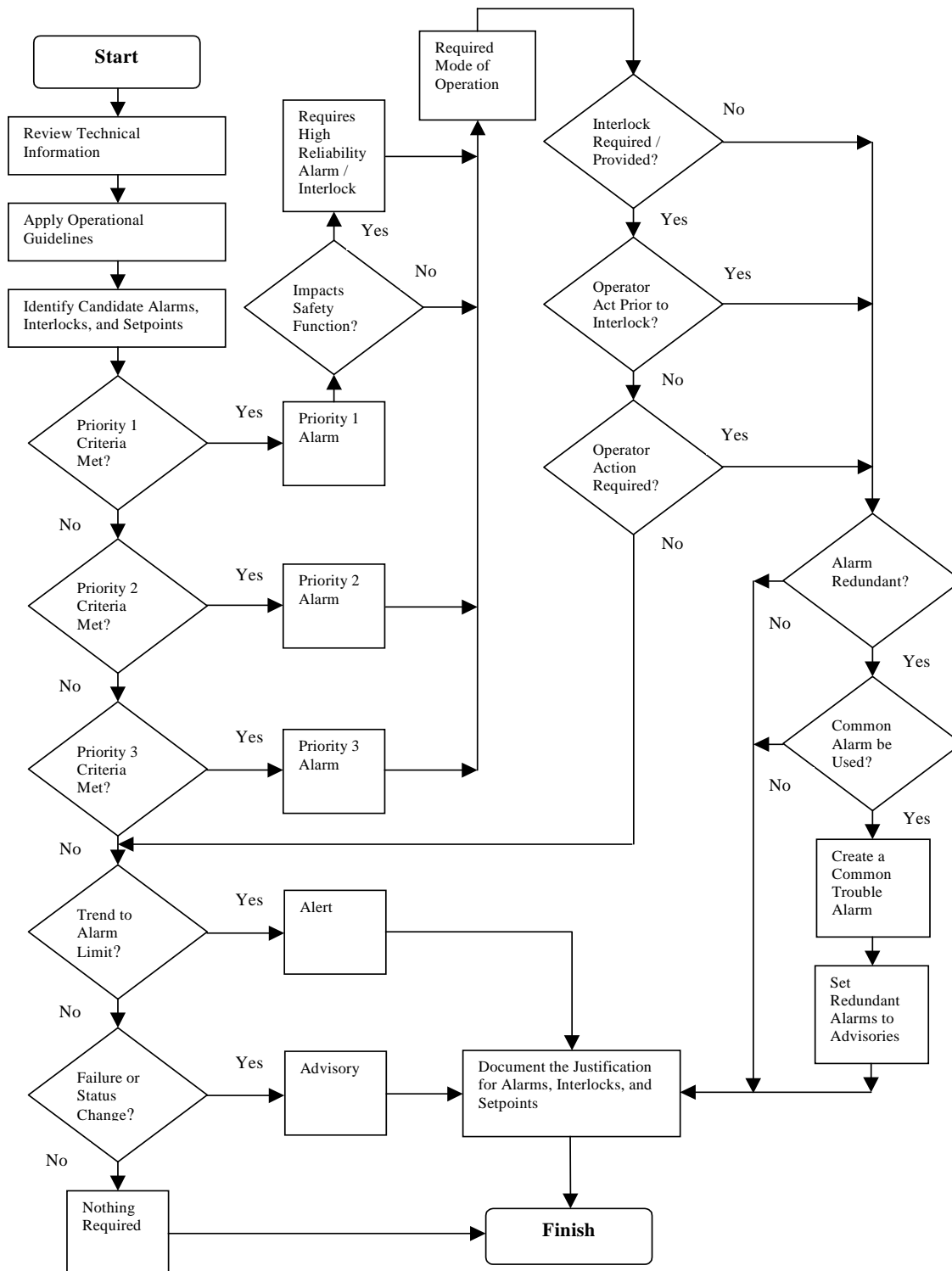
Attachment 2: Alarm Selection Worksheet

Alarm Validation Process Procedure # _____ Rev. _____ Date: _____

1	Equipment No.: CLI No.: Type of Instrument Loop: DCS PLC Hardwire Other: _____
2	Process System Loop Description: (Descriptive Title of Instrument Loop and Variable)
3	Alarm Setpoint: (Value and Engineering Units) Set Point Type: (Example: High-High, Low-Low)
4	Interlock Required: (Identify Interlock Requirements)
5	Alarm Priority Level: (Determined by the Validation Process) Priority 1 Priority 2 Priority 3 Alert Advisory None
6	Applicable Modes of Facility Operation and Maintenance: (Example: Startup, Steady State Operation, Two Trains Running)
7	Recommended Changes Resulting from Validation Process:
8	Description of Alarm Functionality and Required Operator Alarm Response:

Facility Operations Manager Approval _____ Date: _____

Design Authority Approval _____ Date: _____

Alarm Review Team Approval _____ Date: _____

Attachment 2: Alarm Selection Worksheet

INSTRUCTIONS:

The Design Authority Engineer should enter the number and revision level of the Alarm Validation Procedure, the date the review was completed, and fill in the information in Sections 1 through 8 of the Alarm Selection Worksheet as described below for each alarm / interlock:

Section 1:   Enter the CLI and EN number for the component generating the alarm / interlock. Indicate how the alarm / interlock is implemented (e.g., DCS, PLC, or Hardwire).

Section 2:   Enter a description of the process and the measured variable (e.g., HEPA Filter Pressure Drop).

Section 3:   Enter the set point value and type (e.g., Setpoint = 30°C, High / Low Alarm).

Section 4:   If an interlock is involved, describe the interlock action.

Section 5:   List the priority as determined by the Alarm Validation Process.

Section 6:   List the operating and maintenance modes that the alarm or interlock should be active.

Section 7:   Document proposed changes resulting from the Alarm Validation Process (i. e. delete, make an advisory, hardwire, change priority, make common alarm).

Section 8:   Document the alarm functionality and required operator alarm response.

After completing the information, the Design Authority Engineer will sign the Alarm Selection Worksheet and submit it to his manager for review.

The Design Authority Engineering Manager will submit completed Alarm Selection Worksheets to the Alarm Review Team for review and approval.

If the Alarm Validation Process affects an existing facility, then the Design Authority Engineering Manager will submit the Alarm Selection Worksheets to the Facility Operations manager for review and approval.